日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１０月２１日

出願番号
Application Number: 平成１１年特許願第２９９６３５号

出願人
Applicant (s): 松下電器産業株式会社

２０００年 ３月 ３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０１２９０１

【書類名】　特許願

【整理番号】　2032410357

【提出日】　平成11年10月21日

【あて先】　特許庁長官殿

【国際特許分類】　G11B　7/007

G11B　7/00

G11B　7/09

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　永井　隆弘

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　石原　秀志

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　伊藤　基志

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録方法、光ディスク再生方法、データ処理方法及び情報処理システム

【特許請求の範囲】

【請求項１】　著作権保護を必要とするＡＶデータを含むデータを記録する記録型光ディスクであって、

前記記録型光ディスクはセクタ構造を有し、

前記セクタはセクタヘッダ領域と暗号化された前記ＡＶデータを含むデータを記録するメインデータ領域を有し、

前記セクタヘッダ領域には著作権制御情報領域と暗号化された前記ＡＶデータを含むデータを復号するために必要な復号鍵情報領域を有し、

前記復号鍵情報領域のサイズは前記復号鍵より小さいことを特徴とする光ディスク。

【請求項２】　前記ＡＶデータを含むデータに施された暗号を復号するための復号鍵が所定のサイズに分割され、連続する前記セクタの前記復号鍵情報領域に記録される請求項１に記載の光ディスク。

【請求項３】　前記復号鍵の分割数は、エラー訂正に必要なセクタであるＥＣＣブロックに含まれるセクタ数の約数である請求項２に記載の光ディスク。

【請求項４】　連続するセクタに分割された復号鍵を記録する復号鍵領域を有するセクタにおいて、

前記ＡＶデータを含むデータのサイズが（メインデータサイズ）×（復号鍵の分割数）に満たないメインデータ領域に、ダミーデータを有する請求項２または３記載の光ディスク。

【請求項５】　前記ＥＣＣブロックにおいて、連続するセクタに分割された復号鍵を記録した復号鍵領域を有するセクタが、（ＥＣＣブロック単位）／（復号鍵の分割数）回記録され、前記ＡＶデータを含むデータのサイズが（メインデータサイズ）×（ＥＣＣブロック単位）に満たないメインデータ領域に、ダミーデータを有する請求項３または４記載の光ディスク。

【請求項６】　前記ＡＶデータを含むデータに施された暗号を復号するための

復号鍵が複数の復号鍵領域を有する復号鍵領域復号鍵テーブルに記録され、メインデータ領域に記録された前記ＡＶデータを含むデータに施された暗号を復号するための前記復号鍵領域を参照するためのインデックスが前記セクタの前記復号鍵情報領域に記録される請求項１に記載の光ディスク。

【請求項７】　前記ＡＶデータを含むデータに施された暗号を復号するための復号鍵が所定のサイズに分割され、前記復号鍵テーブルの連続する複数の前記復号鍵領域に記録される請求項６に記載の光ディスク。

【請求項８】　前記復号鍵テーブルは書換え可能なリードイン領域内のメインデータ領域に記録されることを特徴とする請求項６または７に記載の光ディスク。

【請求項９】　復号鍵テーブルの記録状態を表す情報が、復号鍵テーブルの各復号鍵領域に固定値として記録される請求項６または７に記載の光ディスク。

【請求項１０】　復号鍵テーブルの記録状態を表す情報として、復号鍵テーブルの各復号鍵領域に対する復号鍵状態を記録した復号鍵状態領域が記録される請求項６または７に記載の光ディスク。

【請求項１１】　前記復号鍵テーブルは、異なる前記ＥＣＣブロックに複数回記録される請求項８に記載の光ディスク。

【請求項１２】　前記復号鍵テーブルは、ディスクの内外周に配置された異なる前記ＥＣＣブロックに複数回記録される請求項８に記載の光ディスク。

【請求項１３】　ファイル管理領域で管理されるファイル単位もしくはディスク上で連続するセクタからなるエクステント単位で前記復号鍵が割り当てられる請求項６または８または１２に記載の光ディスク。

【請求項１４】　ＡＶデータを含むデータを記録するメインデータ領域は、前記データが非暗号化状態で記録される非暗号化領域と、暗号化状態で記録される暗号化領域からなり、非暗号化領域には復号鍵の変換に用いられる復号鍵変換データを有し、暗号化領域のデータは復号鍵変換データを用いて変換された復号鍵により暗号化されていることを特徴とする光ディスク。

【請求項１５】　ＡＶデータを含むデータを記録するメインデータ領域は、ＡＶデータの再生制御に用いられる制御情報が非暗号化状態で記録される制御情報

記録セクタと、ＡＶデータが暗号化状態で記録されるＡＶデータ記録セクタからなり、制御情報記録セクタには復号鍵の変換に用いられる復号鍵変換データを含み、ＡＶデータ記録セクタのＡＶデータは復号鍵変換データを用いて変換された復号鍵により暗号化されていることを特徴とする請求項１４に記載の光ディスク。

【請求項１６】　ＡＶデータ記録セクタはＡＶデータが非暗号化状態で記録される非暗号化領域と暗号化状態で記録される暗号化領域からなり、非暗号化領域には第２の復号鍵変換データを含み、暗号化領域のＡＶデータは復号鍵変換データを用いて変換された復号鍵をさらに第２の復号鍵変換データを用いて変換された復号鍵により暗号化されていることを特徴とする請求項１５に記載の光ディスク。

【請求項１７】　前記復号鍵変換データは、少なくともＡＶデータのコピー制御情報を含む請求項１４に記載の光ディスク。

【請求項１８】　著作権保護を必要とする前記ＡＶデータを含むデータを光ディスクに記録する方法であって、

前記光ディスク上に記録された復号鍵ステータスを読み出し、復号鍵の空き領域を調べるステップと、

空き領域がある場合に復号鍵領域の予約、もしくは復号鍵の記録を行うステップと、

ファイルあるいはエクステント単位での著作権制御情報と復号鍵インデックスを設定するステップと、

復号鍵で暗号化されたファイルもしくはエクステントを記録するステップと、

ファイル管理情報を記録するステップと、

を含むデータ処理方法。

【請求項１９】　著作権保護を必要とする前記ＡＶデータを含むデータを光ディスクから再生する方法であって、

再生するファイルもしくはエクステントの記録領域から復号鍵インデックスを取得するステップと、

前記復号鍵インデックスに対応した復号鍵を取得するステップと、

復号鍵で暗号化されたファイルもしくはエクステントを再生するステップと、
を含むデータ処理方法。

【請求項２０】　著作権保護を必要とする前記ＡＶデータを含むデータを光ディスクから削除する方法であって、

削除するファイルもしくはエクステントの記録領域から復号鍵インデックスを取得するステップと、

前記復号鍵インデックスに対応した復号鍵ステータスを更新し復号鍵を開放するステップと、

ファイル管理情報からファイルエントリを削除し、ファイル管理情報を更新するステップと、
を含むデータ処理方法。

【請求項２１】　著作権保護を必要とする前記ＡＶデータを含むデータを復号鍵で暗号化するデータ暗号化装置と、

前記データを復号するために必要な復号鍵を光ディスクに記録再生する光ディスク記録再生装置と、

前記光ディスク記録再生装置へのデータ及び復号鍵の記録再生を制御する制御装置と、を備えた情報処理システムであって、

前記光ディスク記録再生装置は、

復号鍵ブロックを記録再生する手段と、

前記復号鍵をバス暗号化・復号化し、前記制御装置とデータ転送する手段と、

復号鍵ステータスブロックを記録再生する手段と、
を備えており、

前記制御装置は、

ＡＶデータを含むデータを暗号化した前記データ圧縮装置からバス暗号化されたバス暗号化復号鍵を受信する手段と、

前記復号鍵ステータスブロックから空き領域を調べる手段と、

前記空き領域に前記バス暗号化復号鍵を割り当て、前記光ディスク記録再生装置に転送する手段と、
を備えており、

前記データ暗号化装置から取得したバス暗号化復号鍵を前記制御装置でバス復号することなく、前記光ディスク記録再生装置から取得した前記バス暗号化復号鍵ブロックの開き領域に割り当て、前記光ディスク記録再生装置においてバス復号化した後に光ディスクに記録する情報処理システム。

【請求項２２】　前記データ暗号化装置と前記光ディスク記録再生装置は相互認証方式によりバス鍵の共有を行うことを特徴とする請求項２１に記載の情報処理システム。

【請求項２３】　著作権保護を必要とする前記ＡＶデータを含むデータと前記データを復号するために必要な復号鍵を光ディスクから再生する光ディスク再生装置と、

前記光ディスク再生装置からのデータ及び復号鍵の再生を制御する制御装置と、

前記復号鍵によりＡＶデータを含むデータを復号するデータ復号化装置と

を備えた情報処理システムであって、

前記光ディスク再生装置は、

復号鍵ブロックを再生する手段と、

前記復号鍵をバス復号化し、前記制御装置とデータ転送する手段と、

復号鍵ステータスブロックを再生する手段と、

を備えており、

前記制御装置は、

ＡＶデータを含むデータを復号化するバス暗号化復号鍵を前記光ディスク再生装置から受信する手段と、

前記バス暗号化復号鍵ブロックから前記ＡＶデータを含むデータを復号化するために必要なバス暗号化復号鍵を抜き出す手段と、

前記バス暗号化復号鍵を前記データ復号化装置に転送する手段と、

を備えており、

前記データ復号化装置は、

前記暗号化復号鍵を復号化し、復号鍵を生成する手段と、

前記復号鍵により前記ＡＶデータを含むデータを復号化する手段と、

を備えており、

前記光ディスク再生装置から取得したバス暗号化復号鍵ブロックを前記制御装置でバス復号することなく、前記ＡＶデータを含むデータを復号化するためのバス暗号化復号鍵を取得し、前記データ再生手段においてバス復号化した後にＡＶデータを含むデータの復号化を行いデータを再生する情報処理システム。

【請求項２４】　前記データ復号化装置と前記光ディスク記録再生装置は相互認証方式によりバス鍵の共有を行うことを特徴とする請求項２３に記載の情報処理システム。

【請求項２５】　著作権保護を必要とするＡＶデータを光ディスクに記録する光ディスク記録装置であって、

光ディスクの非暗号化領域には復号鍵変換データを含むデータを非暗号化状態で記録し、暗号化領域には復号鍵変換データを用いて変換を施した復号鍵によりデータを暗号化して記録することを特徴とする光ディスク記録装置。

【請求項２６】　ＡＶデータの再生制御に用いられる制御情報を制御情報記録セクタに非暗号化状態で記録し、制御情報に含まれる復号鍵変換データを用いて復号鍵を変換し、この変換された復号鍵を用いてＡＶデータを暗号化してＡＶデータ記録セクタに記録することを特徴とする請求項２５に記載の光ディスク記録装置。

【請求項２７】　ＡＶデータ記録セクタの非暗号化領域には第２の復号鍵変換データを含むＡＶデータを非暗号化状態で記録し、暗号化領域には制御情報記録セクタに記録する復号鍵変換データを用いて復号鍵を変換し、この変換された復号鍵をさらに第２の復号鍵変換データを用いて変換した復号鍵を用いてＡＶデータを暗号化して記録することを特徴とする請求項２６に記載の光ディスク記録装置。

【請求項２８】　著作権保護を必要とするＡＶデータを光ディスクから再生する光ディスク再生装置であって、

光ディスクの非暗号化領域に記録されている復号鍵変換データを用いて復号鍵を変換し、この変換された復号鍵を用いて暗号化領域に記録されているデータを復号化して再生することを特徴とする光ディスク再生装置。

【請求項２９】　ＡＶデータの再生制御に用いられる制御情報を制御情報記録セクタから再生し、制御情報に含まれる復号鍵変換データを用いて復号鍵を変換し、この変換された復号鍵を用いてＡＶデータ記録セクタのＡＶデータを復号化して再生することを特徴とする請求項２８に記載の光ディスク再生装置。

【請求項３０】　ＡＶデータ記録セクタの非暗号化領域から第２の復号鍵変換データを再生し、制御情報に含まれる復号鍵変換データを用いて復号鍵を変換し、この変換された復号鍵をさらに第２の復号鍵変換データ用いて変換した復号鍵を用いて暗号化領域のＡＶデータを復号化して再生することを特徴とする請求項２９に記載の光ディスク再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は著作権を有する映画や音楽等のデータに対して、データの著作権保護レベルに応じた暗号を利用することができるようにした光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録方法、光ディスク再生方法、データ処理方法及び情報処理システムに関する。

【０００２】

【従来の技術】

従来、ビデオ・テープ・レコーダ（ＶＴＲ）やカセット・テープなどの記録媒体に映像や音楽といったアナログ情報をアナログのまま記録している。近年、ミニ・ディスク（ＭＤ）、デジタル・ビデオ・ディスク（ＤＶＤ)などのディスク状の記録媒体に、映像や音楽といったアナログ情報をデジタル化して記録するようになってきている。このような映像や音楽などのデジタル化された情報（以下、ＡＶデータと記す）は、劣化を生じることなく他のメディアに複製が可能であるため、さまざまな著作権保護を行うための技術が導入されている。

【０００３】

ＤＶＤでは、図１２に示すようにディスク上に記録するコンテンツに対して暗号化を行っている。図１２はＤＶＤ－ＲＯＭディスクにおけるユーザデータ領域の構成を説明する図である。図１２に示すように、ユーザデータ領域はセクタへ

ッダ領域１２０１とメインデータ領域１２０２、誤り検出コード１２０３からなる。セクタヘッダ領域１２０１には、セクタの位置を示すセクタアドレス１２０４、メインデータ領域１２０２に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報など）が記録される著作権制御情報１２０５、メインデータ領域に暗号が施されている場合に復号するための復号鍵が記録される復号鍵領域１２０６からなる。また、メインデータ領域１２０２には、主に著作権保護を必要とするＡＶデータなどが暗号化されて記録される。

【０００４】

このようなユーザデータ領域の再生時には、セクタヘッダから暗号化コンテンツの再生に必要な復号鍵を得る。取得した復号鍵を鍵復号器１２０７にて復号し、復号鍵を得ることのできたセクタのメインデータ領域をそれぞれの著作権制御情報１２０５の内容にしたがって、復号器１２０８にて復号鍵によるメインデータ領域の復号を行い、再生可能なデータを得る。

【０００５】

図１２に示した構成による光ディスクでは、パーソナル・コンピュータ（以下、ＰＣと記す）などからメインデータに対する読み出しが可能であるが、復号鍵を記録した領域を正規の認証機能を有する装置しか読み出しできないようにすることにより、不正な複製や海賊版の作成を防止できるようにしている。

【０００６】

【発明が解決しようとする課題】

近年、パソコンが高性能化し、さらにそれらがネットワークに接続されることによって、高性能でかつ、複数台のパソコンによる高速な暗号の解読が行われている。このような解読に対して、より暗号の強度を高めるためには、暗号に使用する鍵の鍵長を拡張することが必要となる。しかしながら、従来から提案されているようなセクタヘッダに復号鍵を記録するような鍵管理方法では、予め決められた長さ（復号鍵領域のサイズ）以下の復号鍵しか記録することができず、将来に暗号の強度を高めるために鍵長を長くできないという課題があった。

【０００７】

本発明は上記した問題に鑑みて、記録するコンテンツの著作権保護のレベルに

応じて暗号強度の設定を可能とする光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録方法、光ディスク再生方法、データ処理方法及び情報処理システムを提供することを目的とする。

【０００８】

また、本発明の他の目的は、著作権保護を必要とするデータを復号化するために必要な復号鍵の信頼性をより高めることにある。

【０００９】

【課題を解決するための手段】

本発明の光ディスクは、著作権保護を必要とするＡＶデータを含むデータを記録する記録型光ディスクであって、前記記録型光ディスクはセクタ構造を有し、前記セクタはセクタヘッダ領域と暗号化された前記ＡＶデータを含むデータを記録するメインデータ領域を有し、前記セクタヘッダ領域には著作権制御情報領域と暗号化された前記ＡＶデータを含むデータを復号するために必要な復号鍵情報領域を有し、前記ＡＶデータを含むデータに施された暗号を復号するための復号鍵が所定のサイズに分割され、連続する前記セクタの前記復号鍵情報領域に記録され、上記目的が達成される。

【００１０】

前記復号鍵の分割数は、エラー訂正に必要なセクタであるＥＣＣブロックに含まれるセクタ数の約数であってもよい。

【００１１】

連続するセクタに分割された復号鍵を記録する復号鍵領域を有するセクタにおいて、前記ＡＶデータを含むデータのサイズが（メインデータサイズ）×（復号鍵の分割数）に満たないメインデータ領域に、ダミーデータを有してもよい。

【００１２】

前記ＥＣＣブロックにおいて、連続するセクタに分割された復号鍵を記録した復号鍵領域を有するセクタが、（ＥＣＣブロック単位）／（復号鍵の分割数）回記録され、前記ＡＶデータを含むデータのサイズが（メインデータサイズ）×（ＥＣＣブロック単位）に満たないメインデータ領域に、ダミーデータを有してもよい。

【００１３】

本発明の光ディスクは、著作権保護を必要とするＡＶデータを含むデータを記録する記録型光ディスクであって、前記記録型光ディスクはセクタ構造を有し、前記セクタはセクタヘッダ領域と暗号化された前記ＡＶデータを含むデータを記録するメインデータ領域を有し、前記セクタヘッダ領域には著作権制御情報領域と暗号化された前記ＡＶデータを含むデータを復号するために必要な復号鍵情報領域を有し、前記ＡＶデータを含むデータに施された暗号を復号するための復号鍵が複数の復号鍵領域を有する復号鍵領域復号鍵テーブルに記録され、メインデータ領域に記録された前記ＡＶデータを含むデータに施された暗号を復号するための前記復号鍵領域を参照するためのインデックスが前記セクタの前記復号鍵情報領域に記録され、上記目的が達成される。

【００１４】

前記ＡＶデータを含むデータに施された暗号を復号するための復号鍵が所定のサイズに分割され、前記復号鍵テーブルの連続する複数の前記復号鍵領域に記録されてもよい。

【００１５】

前記復号鍵テーブルは書換え可能なリードイン領域内のメインデータ領域に記録されてもよい。

【００１６】

復号鍵テーブルの記録状態を表す情報が、復号鍵テーブルの各復号鍵領域に固定値として記録してもよい。

【００１７】

復号鍵テーブルの記録状態を表す情報として、復号鍵テーブルの各復号鍵領域に対する復号鍵状態を記録した復号鍵状態領域が記録してもよい。

【００１８】

前記復号鍵テーブルは、異なる前記ＥＣＣブロックに複数回記録してもよい。

【００１９】

前記復号鍵テーブルは、ディスクの内外周に配置された異なる前記ＥＣＣブロックに複数回記録してもよい。

【００２０】

ファイル管理領域で管理されるファイル単位もしくはディスク上で連続するセクタからなるエクステント単位で前記復号鍵が割り当てられてもよい。

【００２１】

メインデータ領域に記録された前記ＡＶデータを含むデータは、非暗号化領域と暗号化領域に分割され、前記非暗号化領域には復号鍵との組合せにより、暗号化領域を復号する復号鍵変換データを有してもよい。

【００２２】

前記復号鍵変換データは、マクロビジョンフラグ、コピー世代管理情報、など改竄されることを防止したい情報を有してもよい。

【００２３】

本発明のデータ処理方法は、著作権保護を必要とする前記ＡＶデータを含むデータを光ディスクに記録する方法であって、前記光ディスク上に記録された復号鍵ステータスを読み出し、復号鍵の空き領域を調べるステップと、空き領域がある場合に復号鍵領域の予約、もしくは復号鍵の記録を行うステップと、ファイルあるいはエクステント単位での著作権制御情報と復号鍵インデックスを設定するステップと、復号鍵で暗号化されたファイルもしくはエクステントを記録するステップと、ファイル管理情報を記録するステップとを包含し、上記目的が達成される。

【００２４】

本発明のデータ処理方法は、著作権保護を必要とする前記ＡＶデータを含むデータを光ディスクから再生する方法であって、再生するファイルもしくはエクステントの記録領域から復号鍵インデックスを取得するステップと、前記復号鍵インデックスに対応した復号鍵を取得するステップと、復号鍵で暗号化されたファイルもしくはエクステントを再生するステップとを包含し、上記目的が達成される。

【００２５】

本発明のデータ処理方法は、著作権保護を必要とする前記ＡＶデータを含むデータを光ディスクから削除する方法であって、削除するファイルもしくはエクス

テントの記録領域から復号鍵インデックスを取得するステップと、前記復号鍵インデックスに対応した復号鍵ステータスを更新し復号鍵を開放するステップと、ファイル管理情報からファイルエントリを削除し、ファイル管理情報を更新するステップとを含み、上記目標が達成される。

【００２６】

本発明の情報処理システムは、著作権保護を必要とする前記ＡＶデータを含むデータを復号鍵で暗号化するデータ暗号化装置と、前記データを復号するために必要な復号鍵を光ディスクに記録再生する光ディスク記録再生装置と、前記光ディスク記録再生装置へのデータ及び復号鍵の記録再生を制御する制御装置と、を備えた情報処理システムであって、前記光ディスク記録再生装置は、復号鍵ブロックを記録再生する手段と、前記復号鍵をバス暗号化・復号化し、前記制御装置とデータ転送する手段と、復号鍵ステータスブロックを記録再生する手段と、を備えており、前記制御装置は、ＡＶデータを含むデータを暗号化した前記データ圧縮装置からバス暗号化されたバス暗号化復号鍵を受信する手段と、前記復号鍵ステータスブロックから空き領域を調べる手段と、前記空き領域に前記バス暗号化復号鍵を割り当て、前記光ディスク記録再生装置に転送する手段と、を備えており、前記データ暗号化装置から取得したバス暗号化復号鍵を前記制御装置でバス復号することなく、前記光ディスク記録再生装置から取得した前記バス暗号化復号鍵ブロックの開き領域に割り当て、前記光ディスク記録再生装置においてバス復号化した後に光ディスクに記録し、上記目的が達成される。

【００２７】

前記データ暗号化装置と前記光ディスク記録再生装置は相互認証方式によりバス鍵の共有を行行ってもよい。

【００２８】

本発明の情報処理システムは、著作権保護を必要とする前記ＡＶデータを含むデータと前記データを復号するために必要な復号鍵を光ディスクから再生する光ディスク再生装置と、前記光ディスク再生装置からのデータ及び復号鍵の再生を制御する制御装置と、前記復号鍵によりＡＶデータを含むデータを復号するデータ復号化装置とを備えた情報処理システムであって、前記光ディスク再生装置は

、復号鍵ブロックを再生する手段と、前記復号鍵をバス復号化し、前記制御装置とデータ転送する手段と、復号鍵ステータスブロックを再生する手段と、を備えており、前記制御装置は、ＡＶデータを含むデータを復号化するバス暗号化復号鍵を前記光ディスク再生装置から受信する手段と、前記バス暗号化復号鍵ブロックから前記ＡＶデータを含むデータを復号化するために必要なバス暗号化復号鍵を抜き出す手段と、前記バス暗号化復号鍵を前記データ復号化装置に転送する手段と、を備えており、前記データ復号化装置は、前記暗号化復号鍵を復号化し、復号鍵を生成する手段と、前記復号鍵により前記ＡＶデータを含むデータを復号化する手段と、を備えており、前記光ディスク再生装置から取得したバス暗号化復号鍵ブロックを前記制御装置でバス復号することなく、前記ＡＶデータを含むデータを復号化するためのバス暗号化復号鍵を取得し、前記データ再生手段においてバス復号化した後にＡＶデータを含むデータの復号化を行いデータを再生し、上記目的が達成される。

【００２９】

前記データ復号化装置と前記光ディスク記録再生装置は相互認証方式によりバス鍵の共有を行ってもよい。

【００３０】

【発明の実施の形態】

（実施の形態１）

以下、本発明の一実施例実施の形態として、図面を参照して説明する。図１はＤＶＤ－ＲＡＭディスクの書換え可能なユーザデータ領域の構成を説明する図である。図１に示すように、ユーザデータ領域はセクタヘッダ領域１０１とメインデータ領域１０２、誤り検出コード１０３からなる。セクタヘッダ領域１０１には、セクタの位置を示すセクタアドレス１０４、メインデータ領域１０２に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報など）が記録される著作権制御情報１０５、メインデータ領域に暗号が施されている場合に復号するための復号鍵が記録される復号鍵領域１０６からなる。

【００３１】

また、メインデータ領域１０２は、非暗号化１０７と暗号化コンテンツ１０８

に分割され、非暗号化１０７には、ＭＰＥＧにおける同期パターンや各種制御情報など後続するデータの制御情報が記録される。暗号化コンテンツ１０８には主に著作権保護を必要とするＡＶデータなどが暗号化されて記録される。

【００３２】

復号鍵領域１０６には、後続するメインデータ領域１０２を再生するための復号鍵が分割されて記録される。例えば、復号鍵領域４バイトに対して復号鍵が８バイトである場合、復号鍵を４バイトずつ分割し、論理的に連続する２つのセクタの復号鍵領域（１０６、１０９）にそれぞれ記録する。

【００３３】

このようなユーザデータ領域の再生時には、論理的に連続する（欠陥等により使用不可能なセクタはスキップする）複数セクタの復号鍵領域から分割された復号鍵を取得し、必要数を連結器１１１にて連結し、再生に必要な復号鍵を得る。復号鍵を得ることのできたセクタのメインデータ領域をそれぞれの著作権制御情報１０５の内容にしたがって、復号器１１４を用いて復号鍵によるメインデータの復号を行う。

【００３４】

さらに、より暗号の強度を高めるために、復号鍵に対して暗号化を施すことも可能であるし（図中ではディスク鍵により鍵復号器１１２にて復号化）、暗号の結果が一定とならないように、データ中の情報（図中では復号鍵変換データ）を鍵に加えることにより、同一の暗号鍵であっても、異なる暗号結果を提供する（図中では復号鍵変換データにより鍵変換器１１３にて復号化）ことも可能である。なお、復号鍵変換データ１１０には、コピー世代管理情報やアナログのマクロビジョン制御フラグなどの改竄をされることによりデータの不正利用につながるようなデータを利用するのが効果的である。

【００３５】

図２はユーザデータ領域への著作権制御情報と復号鍵領域の配置とメインデータ領域への暗号化コンテンツの配置を示すものである。２０１と２０２の復号鍵領域には２つに分割された復号鍵がそれぞれ配置される。このため、これらのセクタに記録する暗号化コンテンツの大きさによらず、複数のセクタ（図２では２

つのセクタ）が使用されることとなる。この場合、未使用の領域には、ダミーデータが補完される。特に、図２に示したように、１セクタ分の暗号化コンテンツしかない場合には、１セクタ分の補完データ２０３が与えられる。

【００３６】

また、図３はエラー訂正の単位が複数セクタにまたがる場合について示したものである。ＤＶＤの場合、１６セクタをエラー訂正単位（以下、ＥＣＣブロックと記す）としてエラー訂正の能力を高めている。このため、データの記録や再生を行う際にはＥＣＣブロック単位での記録が必要となる。復号鍵を分割する際に任意の数で分割して記録を行ったとすると、復号鍵が複数のエラー訂正ブロックにまたがって記録される場合が発生する。再生の際には、復号鍵の分割されたものすべてを再生する必要があるため、暗号化コンテンツを記録したセクタ以外にも復号鍵を記録した直前のＥＣＣブロックまでも再生する必要がある。図３では復号鍵を分割する数をＥＣＣブロックのセクタ数の約数にすることにより、分割された復号鍵がＥＣＣブロックにまたがって記録されることがなくなる。さらに、１つのＥＣＣブロック内で使用する復号鍵を１種類とし、記録するＡＶデータがＥＣＣブロックに満たない場合には、補完データ、ならびに補完セクタを配置することによって、再生時に不要なセクタをディスクから読み出すことがなくなる。

【００３７】

（実施の形態２）

次に、本発明の他の一実施の形態として、図面を参照して説明する。図４はＤＶＤ－ＲＡＭディスクの書換え可能であるリードイン領域４０１とユーザデータ領域４０２の構成を説明する図である。図１と同様に、リードイン領域４０１とユーザデータ領域４０２はセクタヘッダ領域１０１とメインデータ領域１０２、誤り検出コード１０３を有するセクタからなる。セクタヘッダ領域１０１には、セクタの位置を示すセクタアドレス１０４、メインデータ領域１０２に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報など）が記録される著作権制御情報１０５、メインデータ領域に暗号が施されている場合に復号するための復号鍵を参照するインデックスを記録する鍵インデックス領

域４０３からなる。ユーザデータ領域に記録された暗号化コンテンツを復号するための復号鍵は、テーブル形式で書き換え可能なリードイン領域に記録される（４０４）。鍵インデックス領域４０３に記録されるインデックスによりリードイン領域に記録された復号鍵が参照され、図１の場合と同様にディスク鍵による鍵復号器１１２、復号鍵変換データによる鍵変換器１１３をへて、復号器１１４により暗号化コンテンツの復号を行う。

【００３８】

以上の構成により、セクタヘッダ領域内にある鍵インデックス領域に参照用のインデックスを記録することにより、鍵インデックス領域のサイズとは独立に復号鍵テーブル４０４の復号鍵サイズを割り当てることができる。また、復号鍵サイズを割り当てた後も、鍵インデックスで示される復号鍵テーブル４０４から連続して複数の復号鍵領域を使用することにより、自由なサイズの鍵を利用することができる。

【００３９】

図５はリードイン領域に記録された復号鍵の記録状態について示したものである。（ａ）は復号鍵の初期値（ディスクのフォーマット時などに記録）として、鍵として使用しない既知の固定値（オール０など）５０１を記録し、復号鍵の未記録状態とするものである。（ｂ）は、復号鍵と同様にインデックスにより参照可能なテーブル形式の復号鍵状態テーブル５０２をリードイン領域に配置したものであり、復号鍵の記録状態（未使用、領域予約、鍵記録済など）を示す値が記録される。

【００４０】

図６は復号鍵の信頼性を高めるためにディスク上への復号鍵領域の配置を示すものである。通常、ユーザデータ領域においては欠陥管理が行われるため、書き込み不良が発生した場合には、代替領域等へ交代処理が行われる。しかしながら、リードイン領域では、上記のような欠陥管理は行われない。このため、書き込み不良や読み出し不良等の発生により、ＡＶデータの再生に必要な復号鍵が利用不能となり、さらにはディスクそのものが利用不能となる。したがって、複数のＥＣＣブロックに複数記録しておくことが望ましい。また、近接した領域に複数

が記した場合、傷や埃等により複数記録したものがすべて読めなくなる場合がある。このため、ディスクの内周と外周といったようなレイアウト上離れた位置に記録しておくほうがより好ましい。

【００４１】

なお、本実施の形態では復号鍵領域をリードイン領域に配置した。これは、ユーザデータ領域が通常のリードコマンドやライトコマンドでアクセス可能な領域であることを考慮し、パソコンなどからの安全性を高めるためのものである。したがって、これらをユーザデータ領域に配置しても、同様の効果を得ることができる。

【００４２】

（実施の形態３）

次に、本発明の他の一実施の形態として、図面を参照して説明する。図７はファイルシステムの構造により、所望のファイルが格納されたセクタアドレスを管理する光ディスクの概略図である。

【００４３】

ＩＳＯ１３３４６のファイルシステムの構造では、書換可能型ディスクに対応するため、ファイルの記録位置はファイルエントリと呼ばれる情報を用いて管理される。

【００４４】

例えば、ファイル１（７０３）の記録位置はファイル管理情報領域内のファイルエントリ１（７０１）として格納され、ファイル２（７０４）の記録位置はファイルエントリ２（７０２）として格納される（図７）。ファイルは、ディスク上で連続したセクタの領域を管理するエクステント（７０５、７０６）で構成される。光ディスク上には、ファイルエントリが示す領域に対して実施の形態２で示したような暗号化コンテンツが記録され、また、復号鍵がリードイン領域に属する復号鍵テーブル７０７に記録される。暗号化コンテンツが記録されたセクタのヘッダ領域には、復号に必要な復号鍵の参照用ポインタが鍵インデックス領域７０８に記録される。

【００４５】

上記のようにファイルシステムにより管理される光ディスクにおいて、著作権保護を必要とするコンテンツの記録動作について図８を用いて説明する。

【００４６】

コンテンツの記録の際には、まず、復号鍵テーブルの空き領域を調べる（８０１）。空き領域はない場合には、暗号化コンテンツに対する復号鍵が記録できないために、記録を中止する。空き領域がある場合には、取得済みの復号鍵を記録、また、復号鍵が取得できていない場合には、領域の予約を行う（８０３）。次に、記録するコンテンツの著作権制御情報（暗号化を行うかどうか、暗号化の種類を示す種別、など）と、鍵インデックス領域に記録するインデックスの設定を行い（８０４）、コンテンツを暗号化してディスク上に記録する（８０５）。この時、ファイル単位で同一の著作権制御情報と鍵インデックスを使用してもよいし、エクステント等の単位でこれらを切り替えてもよい。最後に、記録したコンテンツに関する情報をもとに、ファイル管理情報の更新を行う（８０６）。

【００４７】

図９では、図８に示した方法により記録したコンテンツ（ファイル）を再生動作について記述したものである。

【００４８】

ファイルの再生動作を行う際には、再生するファイルが使用している復号鍵テーブルの領域を知るため、ファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ファイル管理情報から再生するファイルのファイルエントリを取得し（９０１）、ファイルエントリにより示される領域のセクタヘッダから鍵インデックス領域の値を取得する（９０２）。エクステント単位で異なる暗号を行っている場合には、それぞれのエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次に、取得した鍵インデックスにより示される復号鍵テーブルの復号鍵領域から復号鍵を取得する（９０３）。その後、ファイルエントリで示される領域からファイル（コンテンツ）読み出し、コンテンツに対して復号する（９０４）。

【００４９】

図１０では、図８に示した方法により記録したコンテンツ（ファイル）を削除

動作について記述したものである。

【００５０】

ファイルの削除動作を行う際には、削除するファイルが使用している復号鍵テーブルの領域を知るため、ファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ファイル管理情報から削除するファイルのファイルエントリを取得し（１００１）、ファイルエントリにより示される領域のセクタヘッダから鍵インデックス領域の値を取得する（１００２）。エクステント単位で異なる暗号を行っている場合には、それぞれのエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次に、取得した鍵インデックスにより示される復号鍵テーブルの復号鍵領域から復号鍵を開放する（１００３）。その後、削除するファイルの書き込み位置を示すファイルエントリをファイル管理情報から削除する（１００４）。従来のファイルシステムでは、ファイルを削除する際にファイルエントリのみの削除を行っていたが、復号鍵と暗号化コンテンツの記録セクタが別れたため、別領域に設けた復号鍵を削除できない。上記では、ファイルエントリの削除に先立ってセクタヘッダ中の鍵インデックスの示す復号鍵を復号鍵テーブルから削除することにより、ディスク上での復号鍵の管理を行っている。

【００５１】

（実施の形態４）

次に、本発明の他の一実施の形態として、図面を参照して説明する。図１１は、光ディスクに著作権保護を必要とするコンテンツを記録／再生する光ディスクシステムの概略図である。図１１の光ディスクシステムは、エンコード装置１１０１、光ディスク装置１１０２、デコード装置１１０３、コンピュータ１１０４の４つの装置を有する。本発明のディスクシステムでは、入力されるＡＶデータ等のコンテンツをＭＰＥＧ等のフォーマットでエンコードし、コンピュータ上でのコンテンツの不正利用を避けるために生成した暗号鍵で暗号化し、光ディスク装置にて光ディスクに記録する。また、光ディスクに記録されているコンテンツを再生し、デコード装置にてコンテンツに対する暗号を復号化し、ＭＰＥＧフォーマットのデコード処理を行い、ディスプレイ等の出力装置に出力する。

【００５２】

エンコード装置１１０１では、ＭＰＥＧエンコードしたコンテンツに対して、暗号鍵により暗号化を行うと同時に、再生時に必要な復号鍵を生成する。光ディスクには、エンコードされたコンテンツと復号鍵を記録する必要があるが、コンピュータ上で復号鍵を平文のまま扱われるような場合には、復号鍵を戻して、暗号化コンテンツの解読が容易になってしまう可能性がある。これを避けるために、エンコード装置と光ディスク装置の間で、相互認証を行うとともに相互に共有したバス鍵を元にバス暗号を行う。これにより、復号鍵はエンコード装置側で、復号鍵の暗号化が施され、光ディスク装置では、暗号化された復号鍵の復号化が行われる。したがって、中間に位置するコンピュータ上では、暗号化された復号鍵のみが取り扱われることになり、一層の安全性が確保されることになる。

【００５３】

光ディスク装置とデコード装置の間でも同様に復号鍵のバス暗号を行うことにより、一層の安全性が確保される。

【００５４】

実施の形態２に示したように、光ディスク上に暗号化されたコンテンツを復号するための復号鍵をテーブル形式で記録するような場合には、光ディスク装置上で再生した復号鍵テーブルをバス暗号化し、コンピュータに転送する。コンテンツ記録時には、コンピュータが平文で光ディスクに記録されている復号鍵状態テーブルから復号鍵テーブルの空き領域を調べ、エンコード装置から転送されるバス暗号化された復号鍵を空き領域に割り当てる。この時、バス暗号として復号鍵単位で完結するような暗号（例えば、復号鍵長単位でのブロック暗号）を用いれば、復号鍵ブロックへの割り当て時に、復号鍵の復号、再暗号する必要がない。

【００５５】

コンテンツ再生時の場合も、光ディスク装置から再生された復号鍵ブロックから再生しようとしているコンテンツの復号化に必要な復号鍵のみをデコード装置へ転送する。この場合も、先の記録時と同様に、バス暗号として復号鍵単位で完結するような暗号（例えば、復号鍵長単位でのブロック暗号）を用いれば、復号鍵ブロックからの復号鍵を抜き取る時に、復号鍵の復号、再暗号する必要がない

。　さらに、復号鍵のサイズを大きくする場合には、光ディスク装置の変更すること無く、復号鍵を複数割り当てるなどの復号鍵領域の拡張がコンピュータ上で容易かつ安全に行うことができる。

【００５６】

なお、実施の形態１と実施の形態２では復号鍵変換データとして暗号化コンテンツが記録されるセクタの非暗号化コンテンツを用いたが、ＡＶデータの再生制御に用いられる再生制御情報を記録する再生制御情報記録セクタのデータを復号鍵変換データとして用いても良い。この場合、コピー制御情報やアナログのマクロビジョン制御フラグなど改竄を防止したいデータを復号鍵変換データとして用いることが容易になる。

【００５７】

さらに、暗号化コンテンツが記録されるセクタの非暗号化コンテンツの一部を第２の復号鍵変換データとし、再生制御情報記録セクタのデータを復号鍵変換データとして復号鍵を変換した結果をさらに第２の復号鍵変換データを用いた変換し、コンテンツを暗号する際の鍵とすることにより暗号の強度を高めることも可能となる。

【００５８】

【発明の効果】

以上詳細に説明したように、本発明の記録型光ディスクは、復号鍵をセクタヘッダ領域に配置された所定サイズの復号鍵領域に分割して記録する、あるいは可変長の復号鍵をセクタヘッダ領域に配置された鍵インデックス領域で示された復号鍵領域に記録可能とすることによって、セクタヘッダ領域にあらかじめ規定されたサイズの復号鍵領域にとらわれることなく、自由な長さの復号鍵を利用できる記録型光ディスクを提供できる。これにより、記録するコンテンツに対する著作権保護レベルに応じて、任意の鍵長を用いた暗号を利用可能とすることができる。

【図面の簡単な説明】

【図１】

著作権保護を必要とするデータを記録する実施の形態１の光ディスクの構成を

示すブロック図

【図２】

同実施の形態１におけるダミーデータを有する復号ブロックの構成を示すブロック図

【図３】

同実施の形態１におけるダミーデータを有するＥＣＣブロックの構成を示すブロック図

【図４】

著作権保護を必要とするデータを記録する実施の形態２の光ディスクの構成を示すブロック図

【図５】

同実施の形態２における復号鍵の記録状態を示すリードイン領域の構成を示すブロック図

【図６】

同実施の形態２における複数の復号鍵領域を設けた光ディスクの構成を示すブロック図

【図７】

ファイルシステムの構造を有する実施の形態３における光ディスクを示すブロック図

【図８】

同実施の形態３におけるコンテンツ記録動作を示す処理フロー図

【図９】

同実施の形態３におけるコンテンツ再生動作を示す処理フロー図

【図１０】

同実施の形態３におけるコンテンツ削除動作を示す処理フロー図

【図１１】

コンテンツの記録再生を行う実施の形態４における光ディスクシステムを示すブロック図

【図１２】

著作権保護を必要とするデータを記録する従来の光ディスクの構成を示すブロック図

【符号の説明】

１０１　セクタヘッダ領域
１０２　メインデータ領域
１０３　誤り検出コード
１０４　セクタアドレス
１０５　著作権制御情報
１０６　復号鍵領域
１０７　非暗号化コンテンツ
１０８　暗号化コンテンツ
１０９　復号鍵領域
１１０　復号鍵変換データ
１１１　連結器
１１２　鍵復号器
１１３　鍵変換器
１１４　復号器
２０１　復号鍵（１／２）
２０２　復号鍵（２／２）
２０３　補完データ
４０１　リードイン領域
４０２　ユーザデータ領域
４０３　鍵インデックス領域
４０４　復号鍵テーブル
５０１　未記録状態データ
５０２　復号鍵状態テーブル
５０３　復号鍵状態領域
７０１　ファイルエントリ１
７０２　ファイルエントリ２

７０３　ファイル１

７０４　ファイル２

７０５　ファイル1のエクステント１

７０６　ファイル２のエクステント１

７０７　復号鍵テーブル

７０８　鍵インデックス領域

１１０　エンコード装置

１１０２　光ディスク装置

１１０３　デコード装置

１１０４　コンピュータ

１２０１　セクタヘッダ領域

１２０２　メインデータ領域

１２０３　誤り検出コード

１２０４　セクタアドレス

１２０５　著作権制御情報

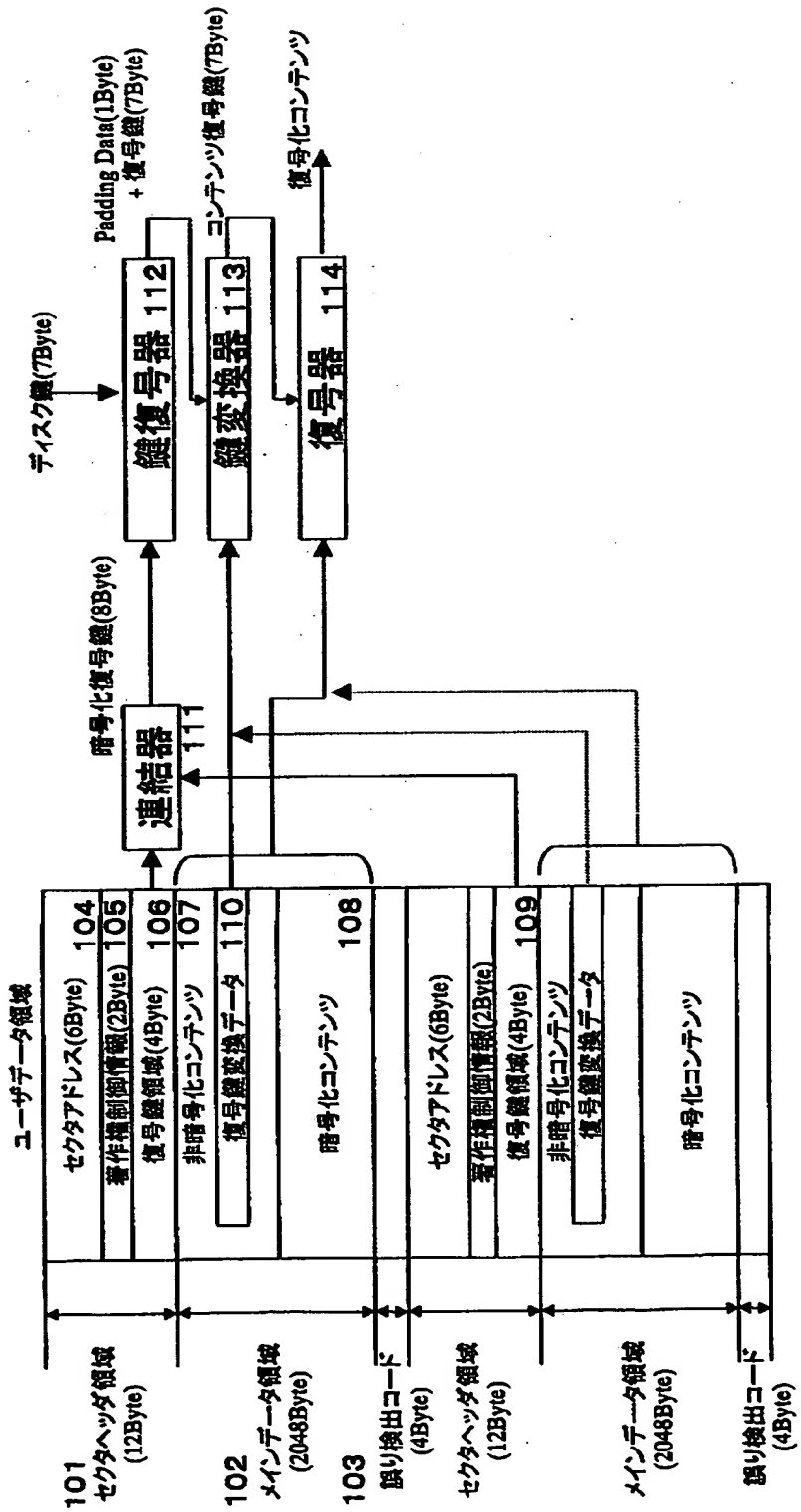
１２０６　復号鍵領域

１２０７　鍵復号器

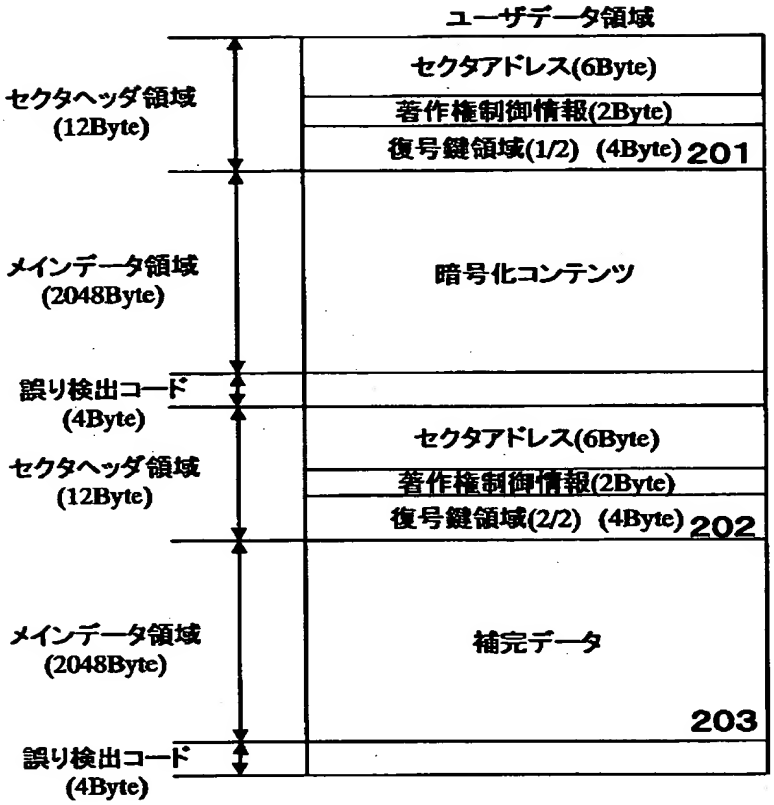
１２０８　復号器

【書類名】　　図面

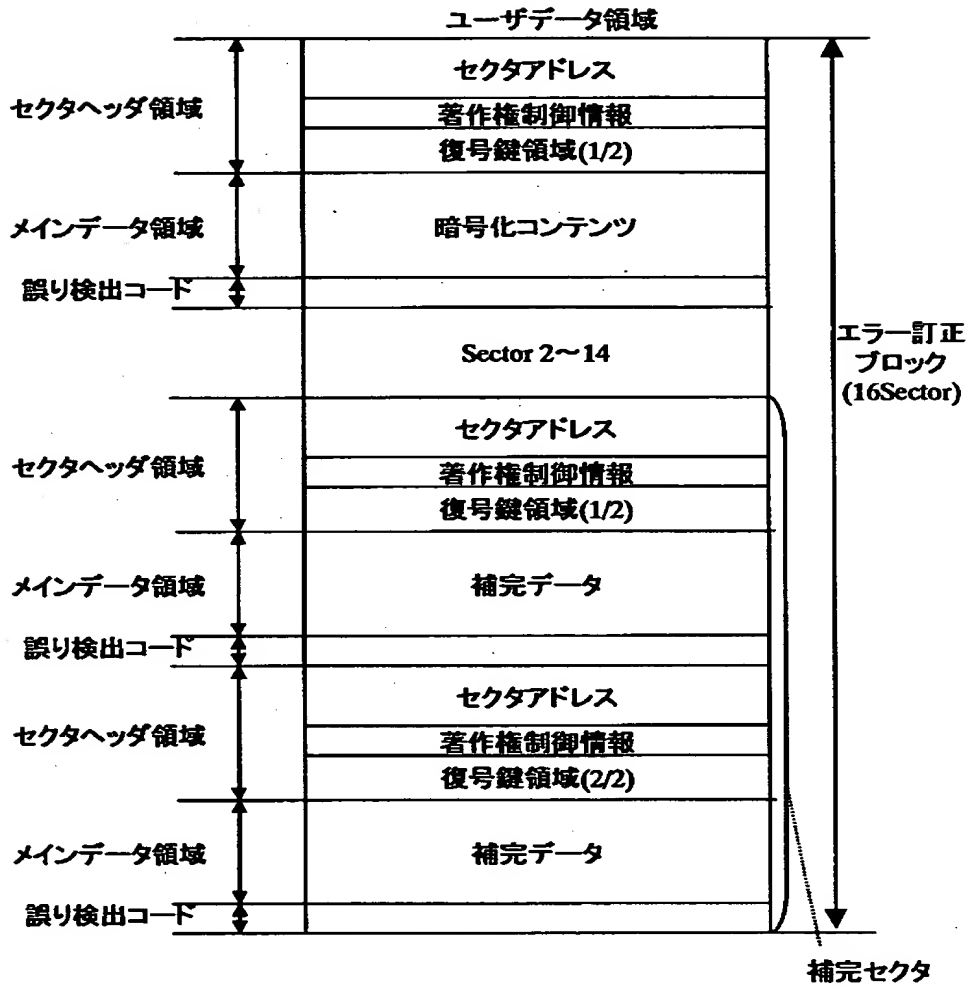
【図１】


ユーザデータ領域
セクタアドレス(6Byte) 104
著作権制御情報(2Byte) 105
復号鍵領域(4Byte) 106
非暗号化コンテンツ 107
復号鍵変換データ 110
暗号化コンテンツ 108
セクタアドレス(6Byte)
著作権制御情報(2Byte)
復号鍵領域(4Byte) 109
非暗号化コンテンツ
復号鍵変換データ
暗号化コンテンツ
101 セクタヘッダ領域 (12Byte)
102 メインデータ領域 (2048Byte)
103 誤り検出コード (4Byte)
セクタヘッダ領域 (12Byte)
メインデータ領域 (2048Byte)
誤り検出コード (4Byte)
暗号化復号鍵(8Byte)
連結器 111
ディスク鍵(7Byte)
鍵復号器 112
Padding Data(1Byte) + 復号鍵(7Byte)
鍵変換器 113
コンテンツ復号鍵(7Byte)
復号器 114
復号化コンテンツ

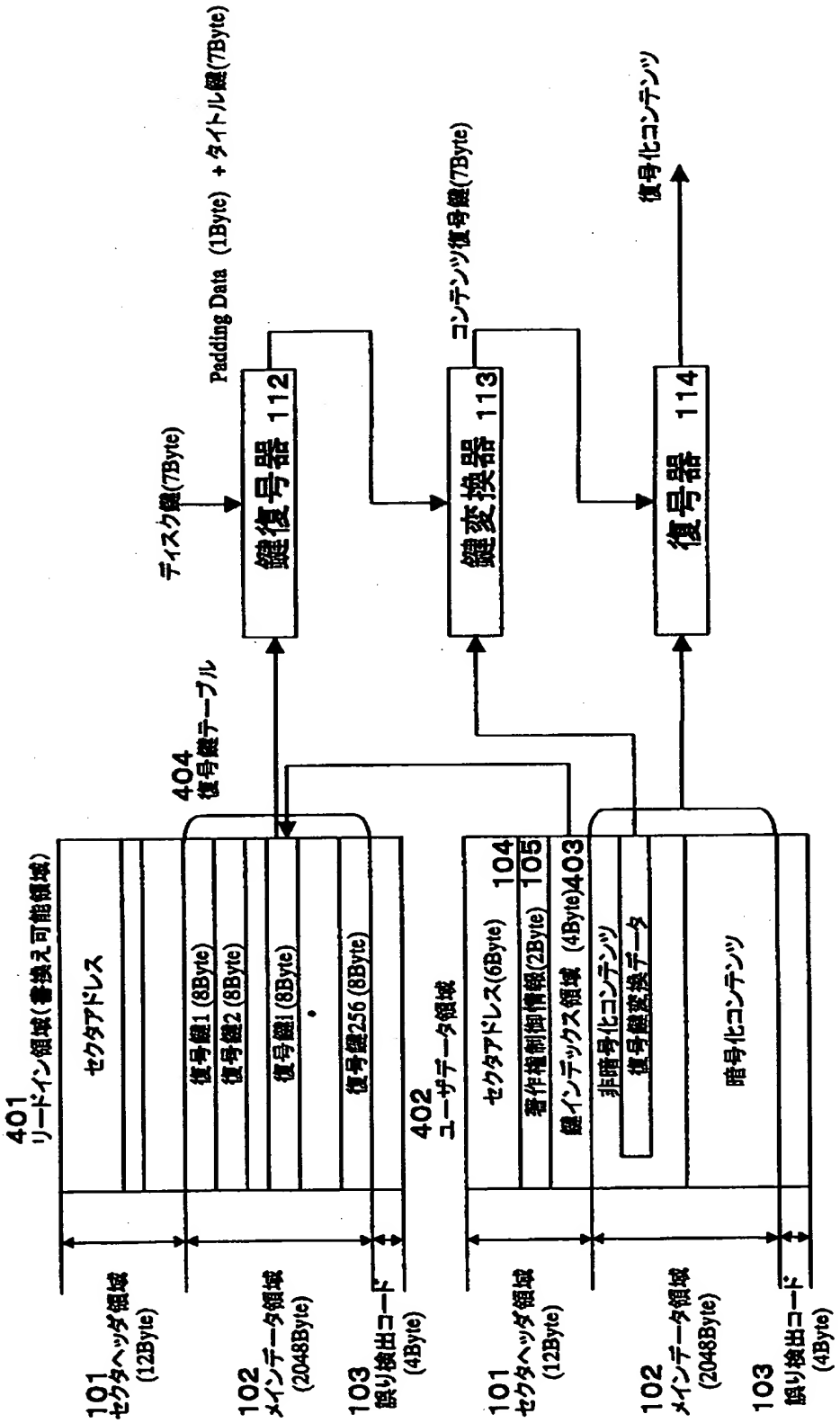
【図２】


ユーザデータ領域
セクタヘッダ領域
(12Byte)
セクタアドレス(6Byte)
著作権制御情報(2Byte)
復号鍵領域(1/2) (4Byte)
201
メインデータ領域
(2048Byte)
暗号化コンテンツ
誤り検出コード
(4Byte)
セクタヘッダ領域
(12Byte)
セクタアドレス(6Byte)
著作権制御情報(2Byte)
復号鍵領域(2/2) (4Byte)
202
メインデータ領域
(2048Byte)
補完データ
203
誤り検出コード
(4Byte)

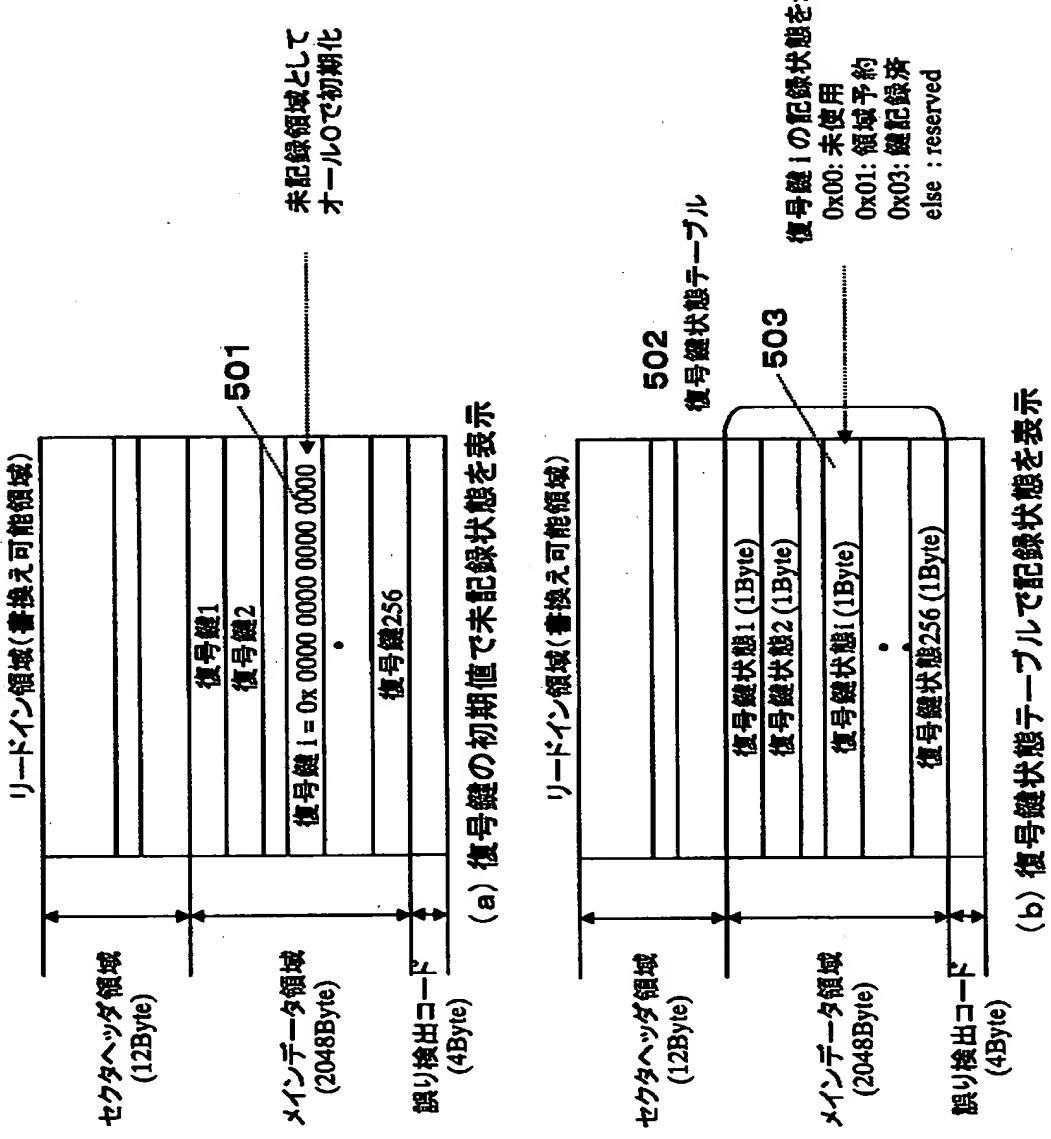
【図３】


ユーザデータ領域
セクタアドレス
著作権制御情報
復号鍵領域(1/2)
セクタヘッダ領域
メインデータ領域
暗号化コンテンツ
誤り検出コード
Sector 2～14
エラー訂正
ブロック
(16Sector)
セクタアドレス
著作権制御情報
復号鍵領域(1/2)
セクタヘッダ領域
メインデータ領域
補完データ
誤り検出コード
セクタアドレス
著作権制御情報
復号鍵領域(2/2)
セクタヘッダ領域
メインデータ領域
補完データ
誤り検出コード
補完セクタ

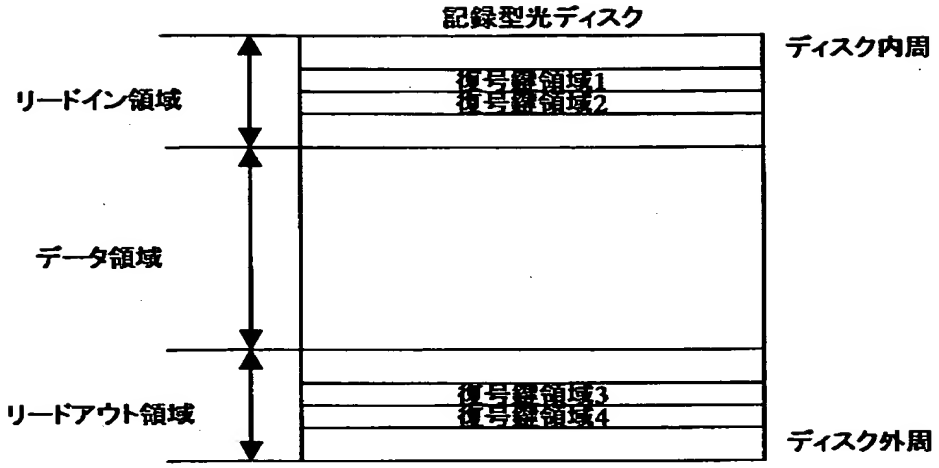
【図４】


ディスク鍵(7Byte)
Padding Data (1Byte) +タイトル鍵(7Byte)
鍵復号器 112
コンテンツ復号鍵(7Byte)
鍵変換器 113
復号化コンテンツ
復号器 114
404
復号鍵テーブル
401
リードイン領域(書換え可能領域)
セクタアドレス
復号鍵1 (8Byte)
復号鍵2 (8Byte)
復号鍵i (8Byte)
復号鍵256 (8Byte)
402
ユーザデータ領域
セクタアドレス(6Byte) 104
著作権制御情報(2Byte) 105
鍵インデックス領域 (4Byte)403
非暗号化コンテンツ
復号鍵変換データ
暗号化コンテンツ
101
セクタヘッダ領域
(12Byte)
102
メインデータ領域
(2048Byte)
103
誤り検出コード
(4Byte)

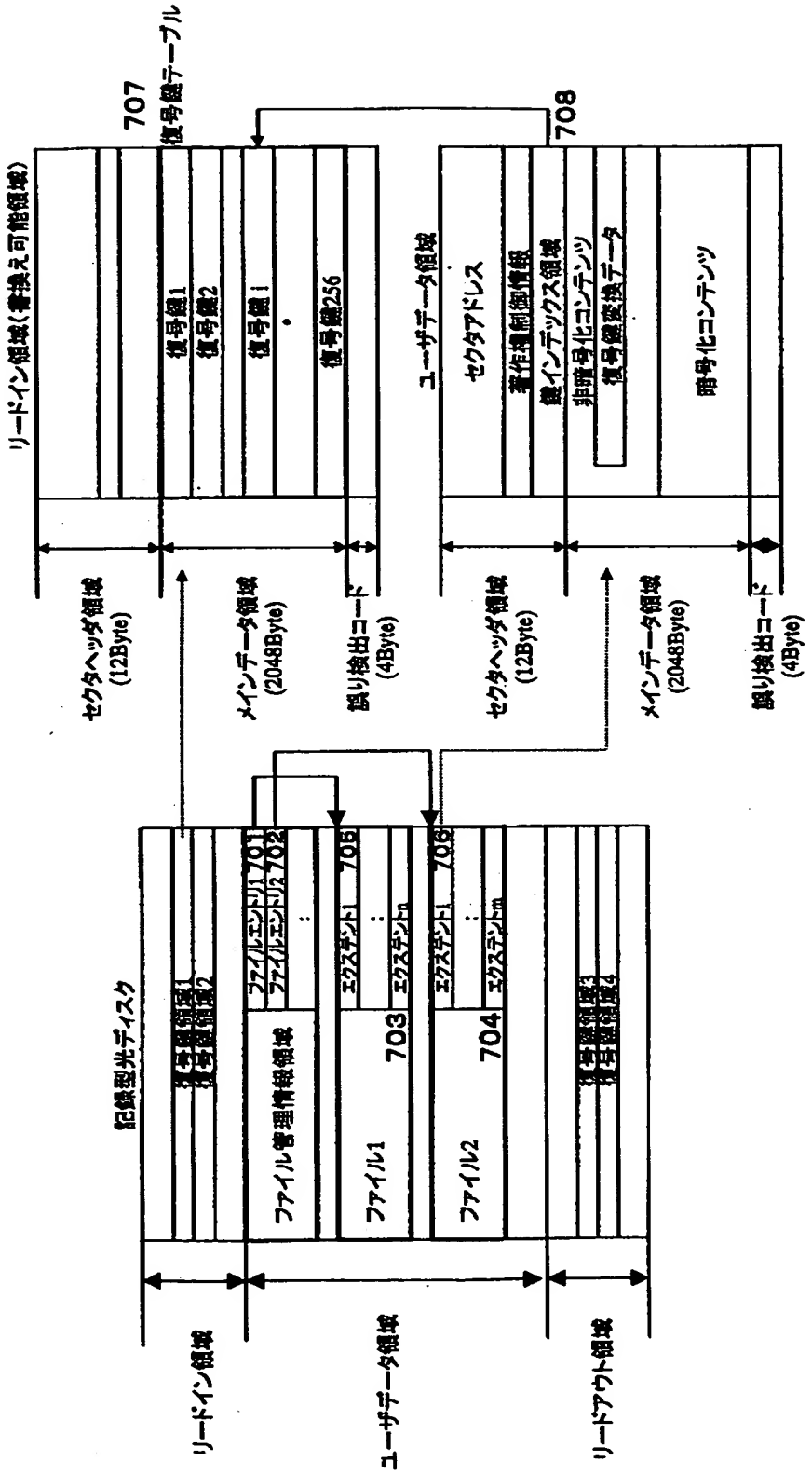
【図５】


リードイン領域(書換え可能領域)
501
未記録領域として
オールOで初期化
復号鍵1
復号鍵2
復号鍵1 = 0x 0000 0000 0000 0000
復号鍵256
セクタヘッダ領域
(12Byte)
メインデータ領域
(2048Byte)
誤り検出コード
(4Byte)
(a) 復号鍵の初期値で未記録状態を表示
リードイン領域(書換え可能領域)
502
復号鍵状態テーブル
503
復号鍵1の記録状態を示す
0x00: 未使用
0x01: 領域予約
0x03: 鍵記録済
else : reserved
復号鍵状態1 (1Byte)
復号鍵状態2 (1Byte)
復号鍵状態i (1Byte)
復号鍵状態256 (1Byte)
セクタヘッダ領域
(12Byte)
メインデータ領域
(2048Byte)
誤り検出コード
(4Byte)
(b) 復号鍵状態テーブルで記録状態を表示

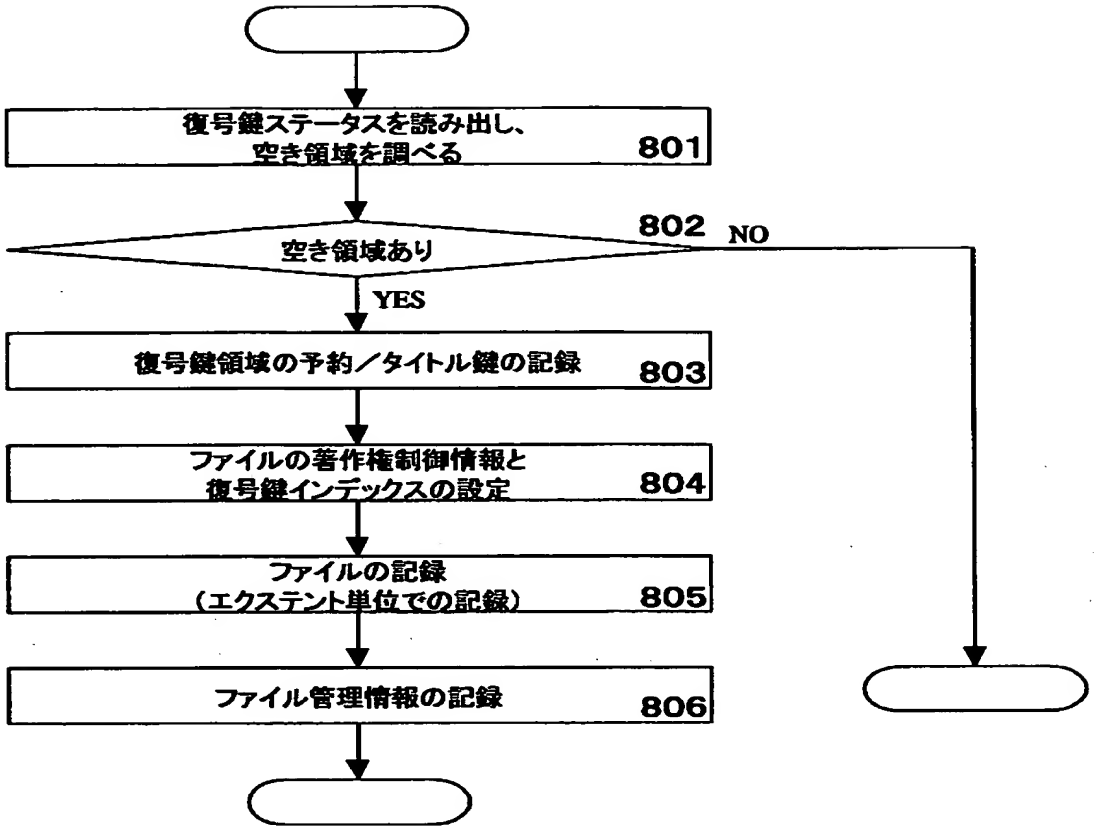
【図６】


記録型光ディスク
ディスク内周
リードイン領域
復号鍵領域1
復号鍵領域2
データ領域
リードアウト領域
復号鍵領域3
復号鍵領域4
ディスク外周

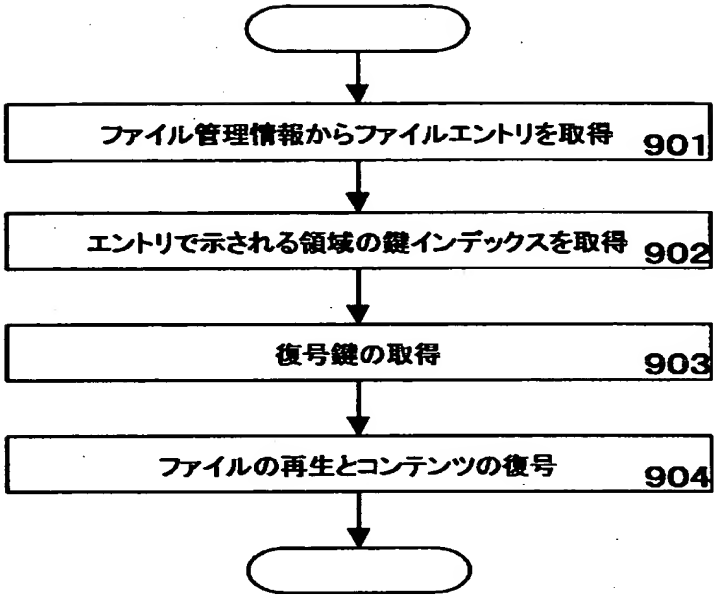
【図７】


707
復号鍵テーブル
708
リードイン領域(書換え可能領域)
復号鍵1
復号鍵2
復号鍵i
復号鍵256
ユーザデータ領域
セクタアドレス
書作権制御情報
鍵インデックス領域
非暗号化コンテンツ
復号鍵変換データ
暗号化コンテンツ
セクタヘッダ領域
(12Byte)
メインデータ領域
(2048Byte)
誤り検出コード
(4Byte)
セクタヘッダ領域
(12Byte)
メインデータ領域
(2048Byte)
誤り検出コード
(4Byte)
記録型光ディスク
ファイル管理情報領域
ファイルエントリ1 701
ファイルエントリ2 702
エクステント1 705
エクステントn
エクステント1 706
エクステントm
ファイル1
703
ファイル2
704
リードイン領域
ユーザデータ領域
リードアウト領域

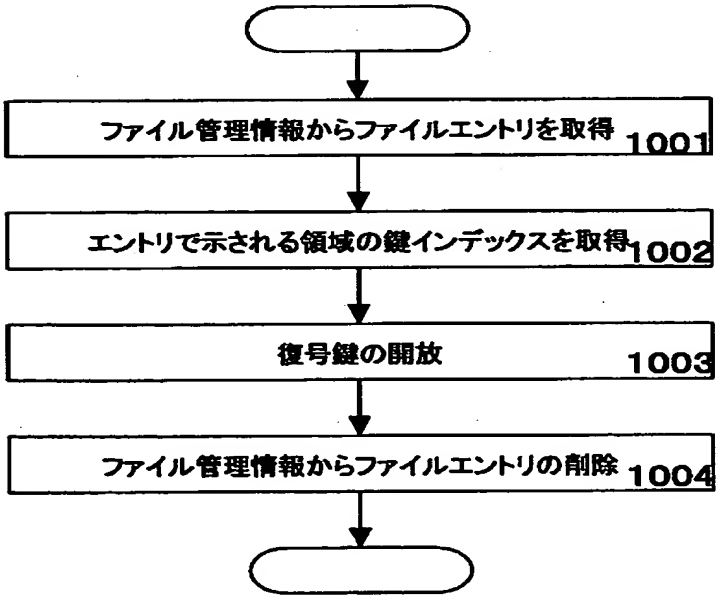
【図８】


復号鍵ステータスを読み出し、
空き領域を調べる
801
802
空き領域あり
NO
YES
復号鍵領域の予約／タイトル鍵の記録
803
ファイルの著作権制御情報と
復号鍵インデックスの設定
804
ファイルの記録
（エクステント単位での記録）
805
ファイル管理情報の記録
806

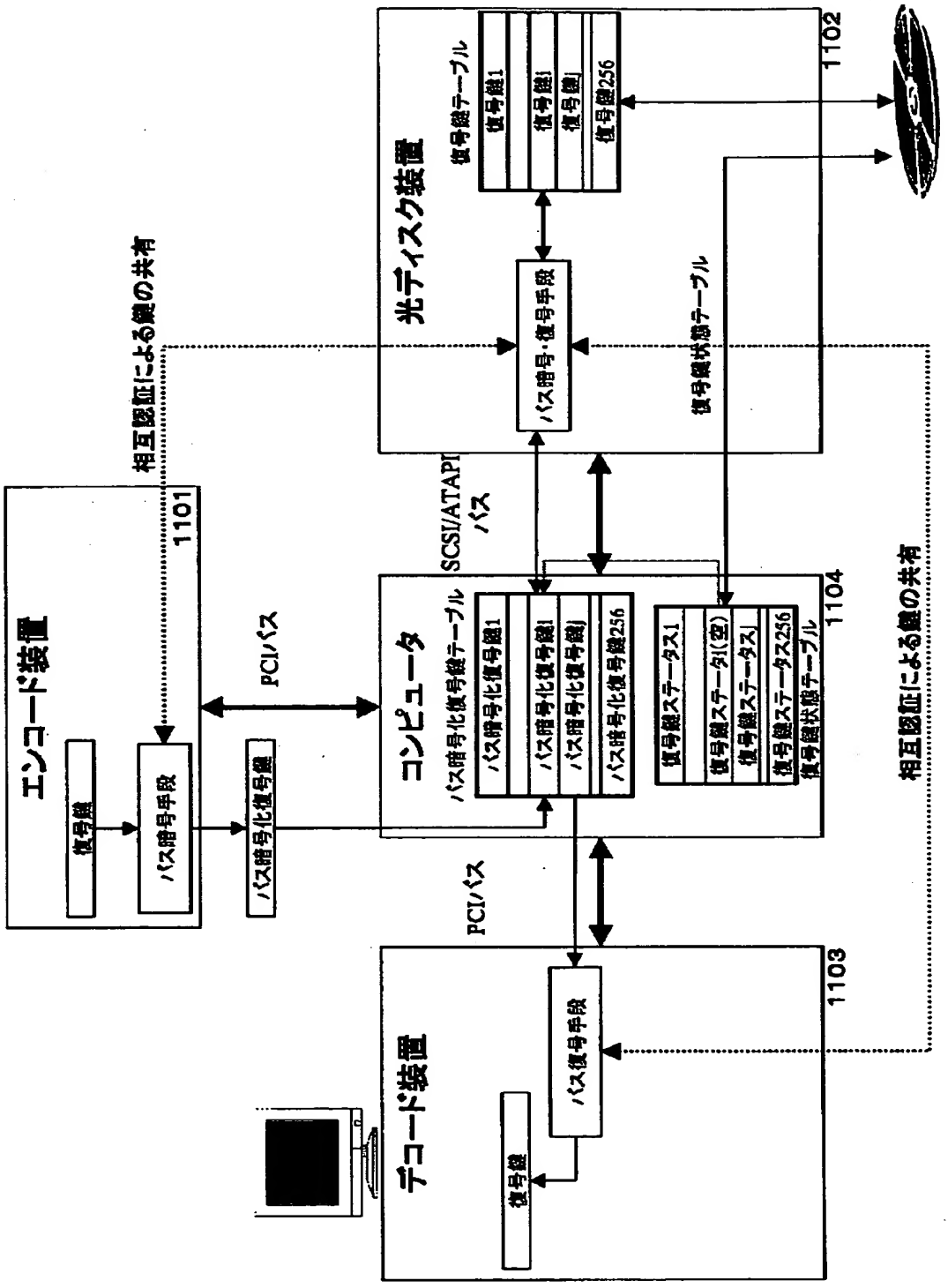
【図９】


ファイル管理情報からファイルエントリを取得
901
エントリで示される領域の鍵インデックスを取得
902
復号鍵の取得
903
ファイルの再生とコンテンツの復号
904

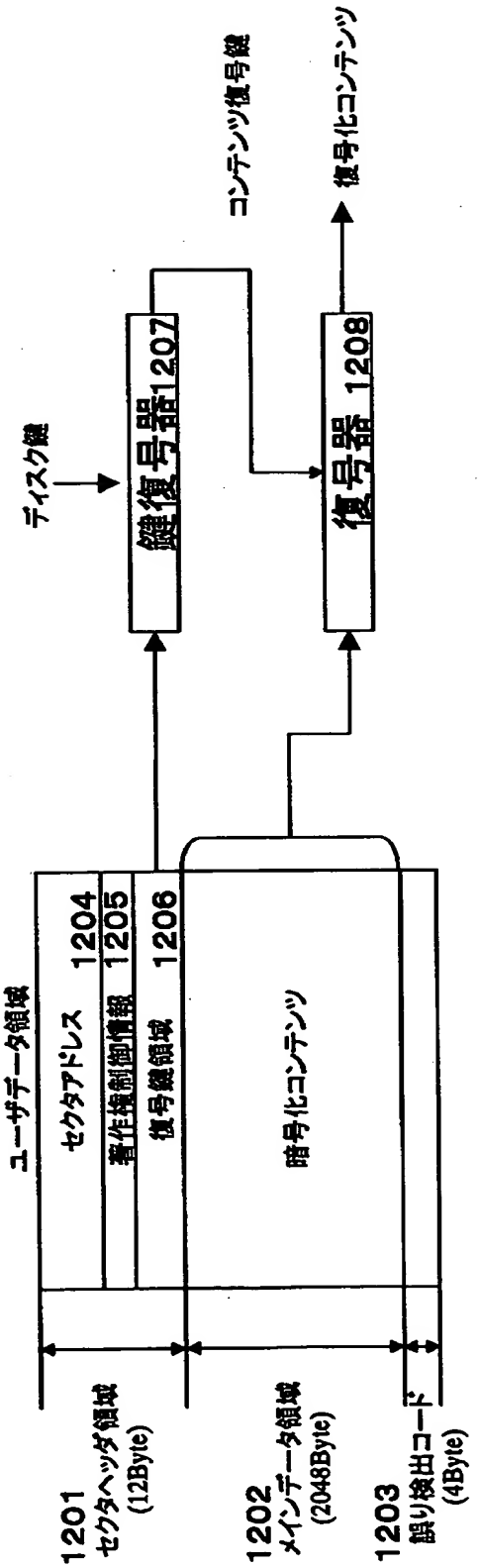
【図１０】


ファイル管理情報からファイルエントリを取得
1001
エントリで示される領域の鍵インデックスを取得
1002
復号鍵の開放
1003
ファイル管理情報からファイルエントリの削除
1004

【図１１】


エンコード装置
1101
復号鍵
バス暗号手段
バス暗号化復号鍵
相互認証による鍵の共有
PCIバス
コンピュータ
バス暗号化復号鍵テーブル
バス暗号化復号鍵1
バス暗号化復号鍵1
バス暗号化復号鍵1
バス暗号化復号鍵256
SCSI/ATAPI
バス
光ディスク装置
1102
復号鍵テーブル
復号鍵1
復号鍵1
復号鍵1
復号鍵256
バス暗号・復号手段
復号鍵状態テーブル
1104
復号鍵ステータス1
復号鍵ステータス(空)
復号鍵ステータス1
復号鍵ステータス256
復号鍵状態テーブル
相互認証による鍵の共有
PCIバス
デコード装置
1103
バス復号手段
復号鍵

【図１２】


ディスク鍵
鍵復号器1207
コンテンツ復号鍵
復号器 1208
復号化コンテンツ
ユーザデータ領域
セクタアドレス 1204
書作権制御情報 1205
復号鍵領域 1206
暗号化コンテンツ
1201
セクタヘッダ領域
(12Byte)
1202
メインデータ領域
(2048Byte)
1203
誤り検出コード
(4Byte)

【書類名】　要約書

【要約】

【課題】　記録するコンテンツに対する著作権保護レベルに応じて、任意の鍵長を用いた暗号を利用可能とする。

【解決手段】　復号鍵をセクタヘッダ領域に配置された所定サイズの復号鍵領域に分割して記録する、あるいは可変長の復号鍵をセクタヘッダ領域に配置された鍵インデックス領域で示された復号鍵領域に記録可能とする。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社